The Values of Money

WILL TYRANNY OR FREEDOM BE IN YOUR DIGITAL WALLET?

J. Christopher Giancarlo and Jim Harper

FEBRUARY 2023

AMERICAN ENTERPRISE INSTITUTE

Executive Summary

In the next dozen years, a new form of money will appear worldwide: central bank digital currencies—government-backed, digital bearer instruments that operate a lot like cash but reside in digital wallets on smartphones and other devices. Unlike the electronic money we now send through banks and payment providers, this kind of money will allow for transactions that are both digital and hand-to-hand, not passing through financial institutions. And unlike current variants of cryptocurrency called "stablecoins," which are operated privately with their value pegged to national currencies, central bank digital currencies will enjoy the full faith and credit of their sovereign issuers, making them equal in value to the paper money they augment or replace. Countries around the globe are actively advancing this new form of sovereign digital currency.

The United States has a chance to lead in this area and advance well-established democratic principles. If a US central bank digital currency is to comport with American values, though, that leadership will require fresh thinking about current US financial surveillance policy. As an important recent report from the White House's technology advisory office makes clear, it is time to reconsider today's privacy-invasive financial surveillance regime and shift to intelligent enforcement. If there is to be American leadership in the digital future of money, the financial surveillance status quo is the wrong foundation to build it on.

The Values of Money

WILL TYRANNY OR FREEDOM BE IN YOUR DIGITAL WALLET?

J. Christopher Giancarlo and Jim Harper

Work on central bank digital currencies (CBDC) is underway around the world. The People's Bank of China (PBOC) has already placed its digital currency, the eCNY, in the hands of over 260 million Chinese citizens. Among other design features, the eCNY will allow China and allied authoritarian governments to surveil and control the economic and financial transactions of billions of people.

CBDCs are digital versions of the banknotes that underlie current monetary systems. They are government-backed representations of value, so they enjoy the full faith and credit of their sovereign issuers, making them equal in value to the paper money they augment or replace. But they are digital. They operate a lot like cash but reside in digital wallets on smartphones and other devices. Unlike the electronic money we now send through banks and payment providers, this kind of money will allow for transactions that are both digital and hand-to-hand. Transferring CBDCs does not require a financial institution's support. Though their use may look a lot like transfers of conventional money administered using a bank or online payment system, the direct and literal transfer of value that CBDCs make possible will be a sea change in the operation of money.

China's eCNY is the first mile marker in the journey to the future of money. China's early and strong lead in the deployment of CBDC raises the question of what form of digital money will be adopted by its economic competitors, including democratic societies. The opportunity exists to counter digital money like the eCNY with an alternative that protects personal privacy and proscribes the potential Orwellian dimensions of both sovereign and non-sovereign digital money. Seizing that opportunity would ensure that future digital currencies—both sovereign examples such as the US dollar or euro and non-sovereign digital currency such as stablecoins—would remain desired and aspirational currencies for generations to come.

That opportunity may be thwarted if the governments of the United States and other developed economies do not part with the window into citizens' financial activity that is provided by current anti–money laundering policies. The White House Office of Science and Technology Policy's (OSTP) recent *Technical Evaluation for a U.S. Central Bank Digital Currency System*[1] shows that financial surveillance in the West is more like China's than many would like to admit. Unwillingness to evolve beyond today's constitutionally suspect financial surveillance system may undermine the opportunity to safeguard economic liberty and expand financial inclusion in the digital future of money.

Coming Soon: CBDCs

CBDCs have taken flight globally. According to the Atlantic Council, 105 countries, representing over 95 percent of global gross domestic product, are exploring a CBDC.[2] Actively engaged in this digital gold rush are 19 of the G20 countries, including India, Japan, Russia, and South Korea, each of which has

made significant recent progress. It is expected that the European Central Bank will introduce a prototype for a "digital euro" by the end of 2023, to become more widely available by 2025.[3]

Of the G7 economies, the United States and United Kingdom are the furthest behind on CBDC development. The old guard of the global currency game—the pound and the dollar—are moving slowly.[4] The Federal Reserve is cautiously exploring the potential benefits and risks of CBDCs from a variety of angles, including through publication of a discussion paper and technological research and experimentation. The Biden administration may be getting things moving. Its 2022 executive order proposed to "prioritize timely assessments of potential benefits and risks [of CBDC] under various designs to ensure that the United States remains a leader in the international financial system."[5]

Among the 10 countries that have rolled out functioning CBDCs, China is the first to deploy one widely. According to Zou Lan, director of the financial market department of the PBOC, an astonishing RMB 87.5 billion ($13.78 billion) in transactions has already been made using China's digital fiat currency.[6] Driving Chinese eCNY adoption is the technology's growing convenience for use in mobile phones and wearable devices[7] and its technological sophistication, given programmability for different consumer and institutional transactions.[8]

A key purpose of the eCNY is to provide China's government with greater control over domestic commerce and visibility into the data it generates. The eCNY bolsters the Chinese government's power over finance, which has been threatened by bitcoin and other non-sovereign digital-currency alternatives. Among China's stated goals for its eCNY are combating domestic corruption, driving greater efficiencies in China's national payment systems, enabling more Chinese people to access the banking system, and conducting greater government oversight and control of business and individual financial transactions.[9] The eCNY will provide Chinese state-owned banks with a more direct window into commercial and personal financial transactions. It will enable the PBOC to directly trace money flows via bank accounts, identity cards, domestic phone numbers, and potentially even foreign phone numbers.

The eCNY is "tiered." It allows anonymous small-value consumer transactions through basic digital wallets obtained without reference to state-issued identity cards. Larger value transactions, however, must be conducted through premium digital wallets linked to bank accounts and individual state-verified identification.[10] Transactions through such wallets support anonymity among transacting parties, including merchants and commercial entities, but full visibility to the PBOC and, hence, the Chinese government.

The deployment of the eCNY complements China's existing electronic surveillance state of police cameras, facial recognition, mobile phones, and electronic-message tracking.[11] Today, China's expanding drone and facial recognition infrastructure can identify an elderly Chinese woman walking without a mask down a central China street and scold her: "Yes, auntie, this drone is speaking to you. You shouldn't walk about without wearing a mask. You'd better go home, and don't forget to wash your hands."[12] With CBDCs, Chinese authorities could follow such warnings with financial punishment: "Auntie, we see you walking about without wearing a mask and have deducted 250 eCNY from your digital wallet. The next time we see you without a mask, you will lose an additional 500 eCNY!"

The eCNY will serve to assign social credit scores and determine who can and cannot petition the Chinese government about grievances.[13] An eCNY user who criticizes the regime may find that their digital money will no longer purchase a train ticket out of their village. A user who pleases the regime may experience greater access and purchasing power—say, better credit terms on a new car. The eCNY will allow the Chinese government to link political conformity to individual prosperity and relegate political dissenters to poverty.

China's eCNY is indeed a benchmark for the future of money, a model that embeds a set of values important to authoritarian governments: surveillance, censorship, and financial controls that thwart dissent and maintain power.[14] This model of currency may be called "surveillance coin."

The eCNY will allow the Chinese government to link political conformity to individual prosperity and relegate political dissenters to poverty.

With tendrils into many developing economies through its Belt and Road Initiative and dominance of 5G technology crucial to wireless payments, China will be a leading exporter of CBDC technology. Surveillance-coin technology will be desired by the world's many regimes that seek its capabilities or countries whose need for Chinese construction of ports and urban infrastructure makes them indifferent to the consequences. China's first-mover advantage in CBDC development threatens to consolidate China's lead in electronic payment technology and shape the global rules and standards for digital finance. Chinese success would elevate authoritarian norms and undermine principles of transparency, accountability, and human rights.

Needed Democratic Response: A Freedom Coin

China's eCNY must not be allowed to set the terms of the world's monetary and financial future. The question for the free world is whether it will foster forms of digital currency—sovereign and non-sovereign—that counter surveillance coin with traditional liberal values such as protection for individual rights, personal privacy, the rule of law, free enterprise, and freedom from censorship. This may be called the "freedom-coin" model of digital currency, featuring well-crafted and affirmatively guarded protections of economic liberty. Such a freedom coin would not merely be less subject to surveillance and censorship compared to a surveillance coin. It would be diametrically and robustly contrary to it.

An effective freedom coin must be built on the premise that privacy is a fundamental social good. It is essential in a free society that respects individuals and their civil rights. In the American constitutional framework, citizens may enjoy privacy—keeping personal information to themselves—for any reason or no reason. Such autonomy over oneself, one's information, and one's financial relationships strengthens and empowers people in many ways, including by preserving their political and legal independence.

Constitutional freedoms of speech, assembly, and worship are often expressed through financial transactions that are easily infringed if not kept private. Privacy—not just consumer privacy but in all transactions—gives people personal autonomy and choice as to how they engage with others and society. Privacy reinforces individual freedom to support controversial causes. Privacy, especially economic privacy, enables a sovereign people to remain sovereign and a free society to remain free.

Privacy Under the US Constitution

Although a right to financial and information privacy is not specifically established by the Fourth Amendment, for the past half century, courts have generally protected individual privacy under a doctrine called the "reasonable expectation of privacy" test. When government agents want to seize or search a person, their house, their papers, or their effects, courts will ask whether doing so violates reasonable expectations.[15]

Disappointingly, this "sociological" approach to constitutional interpretation is not terribly rigorous or protective. The "third-party doctrine," which holds that a person cannot claim constitutional protection for information held by a third party, originated in financial services. The Supreme Court found that government agents could seize and examine a suspect's checks and bank statements without

a warrant because each individual check had passed through a number of hands in the financial services system. Supreme Court justices ranging from Sonia Sotomayor[16] to Neil Gorsuch[17] have questioned the third-party doctrine and the reasonable expectation of privacy test. It is clear that the Court's Fourth Amendment jurisprudence must evolve further in this digital era to renew the balance in a free society between personal privacy and law enforcement.

That Chicken Wire Is a Velvet Rope: Today's Financial Surveillance System

The current financial surveillance regime is known by various combinations of initials—AML for "anti–money laundering," KYC for "know your customer," and CDD for "customer due diligence." Sometimes it's called CFT for "combating the financing of terrorism," a moniker that probably presumes too much about the effectiveness of such programs. We'll call it simply financial surveillance, because that is what it is.

As a practical matter, every bank must know the identity and some basic personal details about its customers to render its services. And the banks must keep track of individual transactions to maintain accounts. But governments have seized on the record-keeping practices of financial services providers, deputizing them to create a huge monitoring operation that covers everyone, not just criminal suspects. Information is collected *in case* someone does something wrong, and not just *when there is probable cause* that someone has done something wrong.

The formal founding of the financial surveillance regime in the United States was the passage of the Bank Secrecy Act (BSA) in 1970.[18] It requires financial institutions to keep records of cash purchases of negotiable instruments, report cash transactions exceeding $10,000, and report suspicious activity. After September 11, 2001, the BSA got a boost, with many more entities required to participate in tracking and reporting Americans' financial transactions. The recipient of this information is the Treasury Department's Financial Crimes Enforcement Network.[19] The Financial Action Task Force,[20] a Paris-based bureaucracy, presses governments worldwide to maintain parallel financial surveillance regimes.

Suspicionless surveillance of everyone's financial transactions is anathema to privacy and American credos such as the presumption of innocence. But the Supreme Court regrettably ratified the practice in a pair of early 1970s cases—*California Bankers Association v. Shultz*[21] and *US v. Miller*.[22] The *Miller* case was the beginning of the above-mentioned third-party doctrine.

Reconsider Financial Surveillance

An examination of BSA is long overdue. The law has been in place for more than 50 years. There has never been a clear and articulate comparison of its costs and benefits;[23] we need to begin that process now.[24] Most benefits are presumed or supported by highly speculative assumptions. As often as not, the question of benefits is chased off by intoning about drug kingpins and terrorists.

Compared to the presumed benefits, the cost of financial surveillance is easier to measure and almost certainly weightier. The Bank Policy Institute found in 2018 that banks it surveyed spent $2.4 billion and employed 14,000 individuals for anti–money laundering regulatory compliance.[25] Worldwide, the cost is easily in the tens of billions of dollars annually. Another part of the cost estimate is the damage done by "de-risking"—the avoidance by financial services providers of certain customers, markets, and even countries. The de-risking of countries may enervate their economies, tax bases, and institutions, putting them in the "failed state" category and perversely imperiling our security.

As a security measure, financial surveillance is somewhat akin to chicken wire. It will help exclude small-time threats. Think of drug distributors as barn cats eyeballing the poultry. The wire may hold off foxes and raccoons for a while, but they will find their way in. It really fails against what matters: large or persistent threats such as bears or burglars coming in the main house.

Given the direct dollar costs, identity requirements, and indirect costs of de-risking, a better analogy for the current financial surveillance regime is a velvet rope. It turns the global financial services system into an exclusive nightclub reserved for the world's wealthy and those endowed with sufficient identity credentials. Financial surveillance excludes under-credentialed people around the globe, people who would benefit most from being able to transact, save, and invest through reliable financial institutions. In a world of eight billion people, roughly a billion and a half do not have access to financial services,[26] often because they do not have identity documents good enough to satisfy financial surveillance requirements.

While disenfranchising many, the existing financial surveillance methodology delivers to banks, law enforcement, and national security agencies enormous amounts of private financial information about innocent people, data troves that have mushroomed since the 9/11 attacks in the US. This financial surveillance "rope line" is increasingly anti-liberal and subject to abuse, even by governments of free societies. It is taking democratic societies closer to the norms of closed societies than is socially acceptable to admit. As the world transitions to digital money—both sovereign and non-sovereign—these policies should be boldly and thoughtfully reconsidered.

Privacy Principles

The Digital Dollar Project is a private sector–led, not-for-profit think tank dedicated to public discussion, research, and pilot testing of the potential advantages and challenges of a US CBDC—or digital dollar.[27] Chaired by this report's coauthor J. Christopher Giancarlo, the project does not call for ready deployment of a US CBDC, but it does advocate that the US assert global leadership in CBDC development and standard setting that is not subordinate to economic competitors and adversaries.

In 2021, the project issued a set of privacy principles to undergird a well-functioning US CBDC.[28] It says a US CBDC must be:

- **Private.** People should be able to use a US CBDC without being subject to undue corporate tracking or government surveillance. People should benefit from aboveboard, contractual sharing of information with providers of financial and other services, or they may refuse it. US law enforcement access to CBDC usage data should be controlled by applicable US law, including the Fourth Amendment.

- **Secure.** A US CBDC should improve and not degrade people's security against theft, hacking, illegal seizure, unauthorized data mining, and fraud. It should provide people with more secure ways to handle money individually, on a system that is secure against attacks and legally protected, with money-handling tools that protect against the frauds that an unfamiliar technology might otherwise allow. A US CBDC should ensure that people's financial data are secure from exploitation by both commercial actors and government authorities.

- **Accessible.** A US CBDC should improve Americans' and global dollar users' access to financial services. Because it is a more efficient system, it should cost less to engage in basic CBDC transactions. And as an open system, it should enhance competition in financial services that produces better services at lower costs.

- **Transparent.** A US CBDC should run on systems that are operationally transparent so that a variety of system users, including the public, can assure themselves independently about its technical functioning, security, and resistance to impermissible monitoring, data mining, and other exploitation.

Each of these four privacy principles could be expanded into a separate, detailed policy prescription. We expand on them to some degree here.

Privacy. The word "privacy" means different things to different people.[29] To the detriment of clarity,

many policy discussions leave it undefined. We consider privacy in this context as the condition people enjoy when they have the power to control information about themselves, exercising that control consistent with their interests and values.[30] Consider the control people have over the appearance of their bodies when they put on clothes. The law of battery lets them do so confident that nobody will remove their clothes and expose them, so bodily privacy is confidently maintained.

In the familiar physical world, we have strong customs, developed over centuries, about whether and how we hide or reveal our bodies, intimate activities, and personal communications. Privacy is more difficult in digital environments because people do not have a clear idea of how information moves over digital networks and because a stable set of norms and standards has not yet emerged.

People maintain privacy most directly by declining to share information at all. Though they may lose some social interactions and conveniences, millions of people live happy, productive lives without using social media and online payments. To get more online benefits and conveniences, people participate in digitized social activity and commerce, protecting privacy by sharing information subject to agreements that control further sharing and use.[31]

These dynamics are easily illustrated in the financial payments context, in which the use of physical cash is an effective protector of privacy. Passing a paper bill from one person to another carries no information with it. A person wishing to keep a purchase private for any number of entirely valid reasons may do so by paying with cash at a store where he or she is unknown. The chance of that person's identity being revealed and recorded, tying the transaction to the individual, is very low. The fact of the transaction almost completely evanesces.

A person with a higher tolerance for information sharing may make purchases with a credit or debit card consistent with his or her privacy preferences. The transfer creates some records, but there are also some protections for privacy written into the terms of service and privacy policy of the payments provider, which bar truly promiscuous information sharing. So a mundane purchase of groceries, for example, produces low-sensitivity information that is well-enough protected by basic policies restricting information to a relatively small orbit around the consumer and payment provider.

A freedom coin should not change—and certainly not weaken—the financial privacy available with today's paper cash.

Privacy is a challenge to the digital future of finance because digitized transfers are "communication events." In a blockchain-based cryptocurrency transaction, the public side of a public-private key pair (the side known as the "wallet") comes to serve as an identifier. Its use is readily observed, and it can be correlated to other wallets, creating pictures of who is transacting with whom. The necessarily public nature of blockchain transactions becomes an open window into financial transactions, which are readily trackable by sovereign and non-sovereign system operators and other sophisticated actors.

In free societies, digital transactions should be designed to not require the sharing of identifiers readily tying transactions to individuals. A freedom coin should not change—and certainly not weaken—the financial privacy available with today's paper cash.

An innovation responding to the identity-revealing feature of the blockchain format is transaction "shielding," which keeps addresses, transaction amounts, and other information hidden from the public, while "zero-knowledge proofs" keep transaction data verifiable by network nodes. Thus, transactions are confirmed without broadcasting

information about them. This makes such transactions roughly analogous in privacy terms to transfers of paper money.

Whether using these techniques or others, a privacy-protective base format for CBDC transactions is essential. Financial services providers adding value by providing security, convenience, and advanced services will require some information from consumers, and they may agree to exchange more. A CBDC that makes information sharing a condition of use, however, would violate the tenet expressed in the Digital Dollar Project principle that there should not be undue corporate tracking or government surveillance.

The small-value privacy "compromise" found in the eCNY and under consideration in many other countries is likely inconsistent with the privacy requirements of a freedom coin. That tiered system would allow anonymity for small-value transactions while maintaining identifiability and tracking for larger transactions. The reason it fails is the likelihood of gaming in such a system, which would inevitably produce a full-surveillance response.

If transactions can be anonymous below a certain threshold, someone wanting to move value privately or illicitly would create multiple accounts and route multiple small transactions through those accounts. Recognizing that avoidance technique, the authorities would likely control the number of accounts or wallets any one person could create. That requires identification of all users and connections between all wallets and users. There is no obvious way to prevent a coin adopting the small-value privacy compromise from rapidly becoming a surveillance coin.

A similar prickly issue is whether a privacy-protective CBDC (or any non-sovereign digital-currency or payment system) should have any provision for government access based on valid warrants and subpoenas. Ideally, one might embed into the base-layer technology a system for exposing transaction data to proper parties when a valid warrant or subpoena requires it. But this is a tremendously difficult engineering and sociopolitical challenge. It would involve provably identifying and credentialing courts in our diverse legal system and creating a secure system for those courts to prove the existence of valid warrants and subpoenas to the technical infrastructure—without opening avenues for attackers to ply that same system. Building a legal disclosure process into the base layer of a transaction-recording system is an enormous challenge that is probably not worth attempting.

A privacy-protective CBDC certainly must not be designed to inject current financial surveillance policies for banks into the money itself. Customer identification requirements, reporting of transactions greater than $10,000, and similar requirements now laid on banks should not be part of the base technical infrastructure. That infrastructure—whether blockchain or some other distributed ledger system—must be able to transfer money opaquely in the system itself, just as dollars are transferred in hand-to-hand transactions without anyone beyond the participants knowing the amounts transacted or the identities of transactors. (Indeed, in anonymous donations, only one side of the transaction knows the identity of both parties.)

Project Hamilton, a multiyear research project of the Federal Reserve Bank of Boston and the Massachusetts Institute of Technology Digital Currency Initiative to explore the CBDC design space and gain a hands-on understanding of a CBDC's technical challenges and opportunities,[32] has made a good start on this.

The project's initial technical release in early 2022 envisioned a system for confirming that financial transactions have happened, rather than recording the content of all transactions. It's a big difference. Confirming the existence of financial transactions without recording their content reduces the amount of data and increases throughput. It also means that private financial data need not be lodged in a centralized ledger where privacy and security risks abound. This protects privacy because use of the system is not conditioned on revealing financial information.

Security. Security is another essential dimension of a successful digital currency. At every layer of the system, from the base transaction infrastructure through user interfaces to users themselves, a digital-currency

system should be at least as secure as the current status quo.

The transaction record-keeping system must be entirely secure. That means it must be essentially impossible for attackers to alter transactions, create counterfeit dollars, spend existing dollars twice, or take the system out of service.

Proof-of-work blockchains such as bitcoin's have a well-established track record of success in this area. Ongoing conversion of energy into cryptographically secured records makes overwriting of the bitcoin blockchain prohibitively costly and essentially impossible. Distribution of the ledger among nodes across the globe makes capture or collusion among nodes prohibitively unlikely. Other forms for securing transaction records, such as proof of stake, may prove out as well.

A US CBDC may rely on trusted institutions to ensure secure record keeping, but that must occur with public verification. The point is to have an authoritative record-keeping system where the existence and accuracy of transaction data are entirely reliable.

The user interfaces must also be secure. Here existing financial services providers are well positioned. Their experience with securing online accounts and online transfers of conventional dollars should translate well to the CBDC environment. Their CBDC services can have the same look and feel as their current dollar services while they tailor their back-end systems to literally transfer dollars. (Online accounts today can be thought of as depicting balances and transfers while masking the complicated administrative processes happening behind the scenes.)

Whether provided by traditional banks or new entrants, the devices and apps that transfer CBDCs directly from digital wallet to digital wallet must help ensure that people are not exposed to thefts and scams. Through various forms of interface design, these tools must assure people they will not be fooled into sending money to impostors or otherwise scammed. People rely on long-standing, almost instinctual habits to protect themselves when they hand over paper dollars from their physical wallets. They will have to learn that a direct CBDC transaction has the same irreversible finality as cash, so they must be aware of and on guard against scams—which are likely in a new CBDC environment—as well as real-world muggers who may force them to surrender funds from their phones.

Security against theft is one thing. Security against illegal seizure is another. A freedom coin CBDC system should not become a new, easier avenue for government agencies to levy fines and punishments without citizen consent, as can be expected from autocratic governments using surveillance coins.

As with transaction data and government surveillance, it is interesting to imagine a base-layer digital-currency system that can administer legal seizure of stolen funds and administer legal penalties, all based on adherence to due process. Yet the challenges in building such a system are prohibitive. The risks of designing such capabilities poorly are too great, and public skepticism about seizure capabilities would likely damn digital-currency projects in democratic societies in the minds of their most important constituencies: their citizens.[33]

Americans have long had a love-hate relationship with their central bank.[34] They would reject giving it the power to take money directly from their wallets.[35] Over generations, as court systems and legal codes are digitized, it may be possible to design a system for directly administering legal processes related to money, but an American CBDC should not wait on such changes. We should not risk planting the seeds of surveillance-coin in the soil of freedom.

Accessibility. We have written of the advantage of existing financial services providers in providing CBDC services. They already have familiar online interfaces and customers who use them. The migration to digital currency, whether sovereign or non-sovereign, should dramatically reduce costs, as the large number of intermediaries now involved in money transfers is reduced. The productivity gains available from reducing middlemen in financial services will benefit many parties—shareholders in the form of increased returns, workers in the form of higher wages, and customers in the form of lower costs and better services. The latter is a policy priority

that a CBDC can help deliver. The traditional financial services system should be accessible to more people who are currently priced out of using it.

The promise of digital-currency programmability will also improve the picture for accessibility. Services better tailored to consumers' needs, created by new firms or established ones, will draw more people into using financial services. CBDC-based financial products will live well within the boundaries of consumer protection law and regulations—and deposit insurance at qualified banks.

Transparency. "Trust, but verify," Ronald Reagan famously said.[36] The claims any CBDC makes to preserve privacy and security will only be real to a free society if they are verifiable and do not rely on trusting in any one institution or government. The privacy and security qualities of the CBDC must be provable to outside reviewers. This essentially means having an open-source system. The computer code that supports transactions must be available to reviewers outside the system—perhaps especially those who are suspicious of it. There can be no reliance on outside parties declared to be trusted. Trust in the system can only be built by showing any observer with the interest and requisite code-reviewing skills that the system does with transaction information what its authors say it does. Of course, transparency in the system's operation is different than making individual transactions transparent.

A relevant extension of this transparency principle is to the institutions involved in the creation and operation of freedom-coin forms of digital currency. The contracts under which technology integrators design or operate a freedom coin must be public. And the public must be assured that no provider of digital-currency infrastructure can turn its superior knowledge into a commercial or political advantage in providing digital-currency-related services.

From Whence Freedom Coin?

Having detailed the concepts of privacy, security, accessibility, and transparency in digital currency, let us now ask what impediments stand in the way of combining them to create a true freedom coin.

A recent report from the OSTP[37] illustrates the conflict between the current approach to financial surveillance and the prospect of US leadership in developing a digital currency that properly protects privacy. OSTP's *Technical Evaluation for a U.S. Central Bank Digital Currency* discusses the many design trade-offs that face US CBDC exploration. For example, should a US CBDC be "permissioned" or "permissionless"? That is, should it allow only approved, permissioned entities to register transactions or make that power available, through cryptography, to anyone controlling some of this new currency? There are trade-offs in terms of privacy, cost of operation, and security.

There is nothing inherently superior about non-sovereign digital currency in protecting individual privacy compared to CBDC.

Across 18 different trade-off sets, OSTP notes repeatedly that CBDC technical and design improvements may hamper the current methodology of AML/CFT. Should a US CBDC system cut out the payments middlemen and the costs they imply? That may hamper AML/CFT. Should a US CBDC use the best possible protections for transaction privacy? That also may hamper AML/CFT. Indeed, several proposals exist in the OSTP report because of financial surveillance policy, such as a "tiered" system in which fully identified users get to transact more readily than those who insist on privacy.

The OSTP report calls existing financial surveillance policy "an imperfect status quo."[38] That is too generous. Rather, it is a significant hindrance to the development of a true freedom coin.

The current practice of financial surveillance impedes the development of a freedom coin by *both* the private and public sectors. In fact, there is nothing inherently superior about non-sovereign digital currency in protecting individual privacy compared to CBDC. It is entirely foreseeable that private-sector sponsors of cryptocurrencies and stablecoins or even commercial servicers of digital dollars, such as wallet providers and others, could be put under political pressure to disable financial transactions with disfavored groups similarly to how many social media platforms, most notably Twitter,[39] have bowed to political winds. They have shifted interpretations of their terms of service to censor a broad range of constitutionally protected speech to appease government officials.[40]

It is easy to imagine that the same social media platforms' terms of service, dictating what ideas can be discussed online, would also determine what activities or political causes can be supported with non-sovereign digital currency.[41] Under political pressure and without being bound by constitutional protections for civil liberties, digital wallet providers might bar transactions with out-of-favor industries, depending on which position's advocates hold political power.[42] Want to give money to a controversial cause such as Planned Parenthood or Right to Life? Want to purchase ammunition or an abortion? You had best check the stablecoin's terms of service and consult its in-house "Office of Community Standards." In democratic societies, lawful transactions in digital money must be immune from political surveillance and censorship regardless of who is in power today, four years from now, and 10 years from now.

Sadly, it is not certain that the public sector would do a better job than the private sector. A fully privacy-preserving CBDC may not soon be digitally minted by the central banks of our Western democratic friends and allies. In a January 2022 speech, the general manager of the Bank for International Settlements (the Swiss-based, central bank to the world's central banks) championed the ability of a sovereign CBDC to provide central banks with visibility into retail financial transactions.[43] Reportedly, the EU is proposing to design its upcoming digital euro with tiering, greater privacy for smaller transactions but government financial surveillance over larger ones.[44]

Lawful transactions in digital money must be immune from political surveillance and censorship regardless of who is in power.

On the US side of the Atlantic, the Federal Reserve's January 2022 CBDC discussion paper indicated that a future digital dollar would protect "consumer" privacy, but not any broader zone of privacy.[45] It may have been a perfunctory word choice, but if the limitation suggests protecting only the privacy of consumer transactions, that leaves much to be desired. It is good that the Federal Reserve does not propose to mine an everyday consumer's shopping history at Walmart. But central banks and governments should not have ready access to citizens' lawful transactions with non-consumer institutions such as Planned Parenthood, National Right to Life, anti-vaccination advocates, the National Rifle Association, or the American Civil Liberties Union—or any other lawful social or political organization whose activities may be in or out of government or social favor.

The OSTP report is a corrective to the Fed's equivocal approach. Among key policy objectives for a US CBDC system, the evaluation included "respect for democratic values and human rights" and, crucially, the need to "maintain privacy and protect against

arbitrary or unlawful surveillance." It states that sensitive financial data should be private and "built-in protections and design choices should ensure that privacy is included by default, including ensuring that data collection conforms to reasonable expectations and only data that is strictly necessary for advancing CBDC system policy objectives is collected."[46]

The OSTP report noted that a US CBDC could leverage privacy-enhancing technologies, such as zero-knowledge proofs, homomorphic encryption, and multiparty computation, that enable parties to prove an encrypted proposition is true without revealing the underlying information.[47] Despite its solicitousness of financial surveillance, the OSTP's CBDC evaluation offers a worthy die for minting freedom coin. We believe more can be done to improve the financial surveillance status quo.

The Financial Freeway: A Better Way of Policing Financial Activity

The unfortunate path of least resistance for digital-currency development could be to simply superimpose the existing financial surveillance infrastructure onto new digital currencies, whether sovereign or non-sovereign. A US CBDC implemented through the two-tiered banking system could coexist with the policy of having banks, fintechs, and other financial institutions and service providers conduct identity verification and surveillance of customers, just as they do today. Criminal enforcement could include the policy of having financial institutions oversee customers and report on them, with the government accessing customer information based on weaker legal standards than the probable cause warrant. The technical design of a US CBDC could facilitate or automatically implement such policies. Yet such an approach only reinforces the privacy-eroding nature of the current financial surveillance system. It is closer to surveillance coin than free and democratic people should accept.

Instead, new digital methods of financial-crime law enforcement may be more effective and certainly less violative of democratic values. In lieu of requiring the collection of detailed data about innocent people in case they later do something wrong, financial-crime control should allow new privacy-shielding technologies and use big data analysis, pattern recognition, and other algorithmic methods to identify wrongdoing if and when it actually takes place.[48]

Technical language should not obscure the commonsense methods we argue for. Take the term "pattern recognition." In the area of credit card payments, it is well recognized that a small purchase of gasoline followed by a large purchase of electronics is consistent with testing to verify that a recently stolen credit card is "live." This behavior pattern—no part of it involving personal identifiers—invites credit card networks to take a closer look and sometimes freeze a card until they can confirm the rightful holder still possesses it. Many more examples use variegated data and follow the latest trends in criminal behavior.

Pattern recognition, not personalized tracking, can raise suspicions that in the law enforcement context may justify investigations that eventually reach into personal information. This approach would allow law enforcement and national security agencies access to digital-currency distributed ledgers to monitor transactions on a pseudonymous basis using modern big data analysis techniques. Think of it as analogous to highway patrol officers monitoring the roadways without tracking each driver's identity. They pull people over when their observations of largely non-personal behavioral information (e.g., speeding) support suspicion of wrongdoing. Further information, including personal identity, would only be accessed from parties holding it based on a neutral magistrate's finding of probable cause—a requirement developed and socially accepted over centuries in our democratic society.

We dub this type of privacy-protective, advanced financial-crime control "intelligent enforcement" (IE). It could be as, if not more, effective in identifying and preventing financial crime than the existing and costly velvet rope approach of AML/KYC financial surveillance. IE would produce far less upfront, personally identified financial information for regulators, law enforcement, and national security agencies

while prompting a shift from today's comprehensive surveillance to more traditional American law enforcement strategies. It would allow greater experimentation and advancement of digital asset technologies with their promise of a more open and inclusive financial system. Perhaps most importantly, it would allow for the development of a true freedom coin that protects the rule of law and individual rights, including personal privacy and free speech.

Conclusion: Freedom Coin as the Foundation for an Enduring US Dollar Reserve Currency Status

The focus of this report has been the erosion of individual freedom by the existing financial surveillance system. It is worse than an "imperfect status quo"[49] for the development of both sovereign and non-sovereign digital currencies. But the flip side of the argument is far brighter: By adopting advanced digital methods of financial-crime control, it will be possible to mint a true freedom-coin form of the US dollar, embodying the principles of privacy, security, accessibility, and transparency we have described.

Development of such an instrument should be seen as an opportunity to reverse the lamentable trend of current financial surveillance and replace it with a new privacy-preserving financial and payment digital architecture. Deployment of such an instrument in a transparent and thus trustworthy manner could engender enormous support among American citizens. Moreover, the inherent and noble characteristics of such a freedom-coin form of digital currency would enhance its comparative value against competing instruments, most notably the surveillance-coin model of authoritarian states.

A US dollar freedom coin would be desirable for people the world over who aspire to financial autonomy and inclusion consistent with basic human rights and true democracy. A freedom-coin design would give a digital dollar a distinct and decided advantage against competing digital currencies—sovereign and non-sovereign—that are less demonstrably protective of personal privacy. Such a design would set up the US digital dollar for generations of reserve currency status in the digital future of money.

The United States has everything to gain by adopting the freedom-coin model of CBDC. It has everything to lose by failing to do so. With thoughtful design choices relating to anonymity and individual privacy, a US CBDC could enjoy superior privacy protections compared to many competing instruments—whether provided by commercial interests or other sovereigns. Coding traditional democratic ideals of economic liberty and privacy into a US CBDC would greatly enhance its global appeal. As it has so often in its history, the US can lead in a way consistent with its finest ideals. But will it lead?

Unwillingness to evolve beyond today's questionable financial surveillance system may undermine the opportunity to safeguard economic liberty and expand financial inclusion in the digital future of money. The OSTP's *Technical Evaluation for a U.S. Central Bank Digital Currency System* helps point the way for democratic governments to reject a surveillance-coin version of CBDC with an alternative freedom coin that protects personal privacy and economic freedom. Seizing that opportunity would ensure that future digital currencies—both sovereign examples such as the US dollar or euro and non-sovereign digital currency such as stablecoins—would remain desired and aspirational currencies for generations to come.

About the Authors

J. Christopher Giancarlo is senior counsel to the international law firm Willkie Farr & Gallagher. He previously served as the 13th chairman of the US Commodity Futures Trading Commission. He is the author of *CryptoDad: The Fight for the Future of Money* (Wiley, 2021). Giancarlo is cofounder and executive chairman of the Digital Dollar Project, a not-for-profit initiative to advance exploration of a US central bank digital currency.

Jim Harper is a nonresident senior fellow at AEI, where he focuses on privacy issues and select legal and constitutional law issues. A lawyer by training, Harper was a founding member of the US Department of Homeland Security's Data Privacy and Integrity Advisory Committee. He is a coeditor of *Terrorizing Ourselves: Why U.S. Counterterrorism Policy Is Failing and How to Fix It* (Cato Institute, 2010) and the author of *Identity Crisis: How Identification Is Overused and Misunderstood* (Cato Institute, 2006).

Acknowledgment

This report represents the views of the authors and does not necessarily reflect the views of the Digital Dollar Project or any of its members, participants, or contributors.

Notes

1. White House, Office of Science and Technology Policy, *Technical Evaluation for a U.S. Central Bank Digital Currency System*, September 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-US-CBDC-System.pdf.

2. Atlantic Council, Central Bank Digital Currency Tracker, 2022, https://www.atlanticcouncil.org/cbdctracker.

3. CBDC Insider, "Legislation for European CBDC Will Be Proposed in 2023," February 11, 2022, https://cbdcinsider.com/2022/02/11/legislation-for-european-cbdc-will-be-proposed-in-2023.

4. Ananya Kumar and Josh Lipsky, "Central Banks Are Embracing Digital Currencies. Will the US Lead or Follow?," Atlantic Council, June 2, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/central-banks-are-embracing-digitall-the-us.

5. White House, "Executive Order on Ensuring Responsible Development of Digital Assets," March 9, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets.

6. China Internet Watch, "China's Digital Currency eCNY Reached 261 Million Digital Wallets," April 25, 2022, https://www.chinainternetwatch.com/33050/cbdc-ecny.

7. Cheng Shi and Gao Xinhong, "E-CNY Signals Digitalization to 'Connect Everything,'" *China Daily*, March 22, 2021, https://global.chinadaily.com.cn/a/202103/22/WS6057f6a8a31024ad0bab0a22_2.html.

8. Wolfie Zhao, "China's New Digital Yuan Test Shows It Can Be Programed to Confine Utility," Block, July 2, 2021, https://www.theblockcrypto.com/post/110377/china-digital-yuan-test-programmable-chengdu.

9. Darrell Duffie and Elizabeth Economy, eds., *Digital Currencies: The US, China, and the World at a Crossroads*, Hoover Institution, 2022, https://www.hoover.org/sites/default/files/research/docs/duffie-economy_digitalcurrencies_web_revised.pdf.

10. Duffie and Economy, eds., *Digital Currencies*.

11. Paul Mozur, Muyi Xiao, and John Liu, "How China Polices the Future: An Unseen Cage of Surveillance," *New York Times*, June 27, 2022, https://www.nytimes.com/2022/06/25/technology/china-surveillance-police.html; and Glitten, "China Deploys Drones, Citizens and Big Data to Tackle Coronavirus," *Wall Street Journal*, March 5, 2020, https://www.wsj.com/video/series/news-explainers/china-deploys-drones-citizens-and-big-data-to-tackle-coronavirus/40590C07-FB56-46CE-8C25-72471A5ECD39.

12. Rachael D'Amore, "'Yes, This Drone Is Speaking to You': How China Is Reportedly Enforcing Coronavirus Rules," Global News, February 11, 2020, https://globalnews.ca/news/6535353/china-coronavirus-drones-quarantine.

13. "The authorities do not seriously solve problems, but do whatever it takes to silence the people who raise the problems." See D'Amore, "'Yes, This Drone Is Speaking to You.'"

14. D'Amore, "'Yes, This Drone Is Speaking to You.'"

15. See *Katz v. United States*, 389 US 347, 361 (1967) (Harlan, J., concurring).

16. Justice Sonia Sotomayor wrote, "It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States v. Jones*, 132 S. Ct. 945, 957 (2012).

17. Dissenting in *Carpenter v. United States*, Justice Neil Gorsuch raised questions about the third-party doctrine, then wrote, "There's a second option. What if we dropped *Smith* and *Miller*'s third party doctrine and retreated to the root *Katz* question whether there is a 'reasonable expectation of privacy' in data held by third parties? Rather than solve the problem with the third party doctrine, I worry this option only risks returning us to its source: After all, it was *Katz* that produced *Smith* and *Miller* in the first place. *Katz*'s problems start with the text and original understanding of the Fourth Amendment." *Carpenter v. United States*, 138 S.Ct. 2206, 2264 (2018).

18. President Richard M. Nixon signed the Bank Secrecy Act, formally the Currency and Foreign Transactions Reporting Act, on October 26, 1970.

19. Financial Crimes Enforcement Network, website, https://www.fincen.gov.

20. Financial Action Task Force, website, https://www.fatf-gafi.org.

21. *California Bankers Association v. Schultz*, 416 US 21, 67, 94 S. Ct. 1494, 39 L.Ed.2d 812 (1974).

22. *US v. Miller*, 425 US 435, 96 S. Ct. 1619, 48 L.Ed.2d 71 (1976).

23. "Although there may be benefits known to international organizations, governments, regulators, and intelligence agencies, no systematic efforts have been made by the FATF network of IOs or countries or institutions to demonstrate benefits. Scientific research on benefits remains in its infancy." Terence C. Halliday, Michael Levi, and Peter Reuter, *Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism*, Center on Law and Globalization, American Bar Foundation, and University of Illinois College of Law, January 30, 2014, 47, https://orca.cardiff.ac.uk/id/eprint/88168/1/Report_Global%20Surveillance%20of%20Dirty%20Money%201.30.2014.pdf.

24. See Norbert J. Michel and Jennifer J. Schulp, "Revising the Bank Secrecy Act to Protect Privacy and Deter Criminals," Cato Institute, July 26, 2022, https://www.cato.org/sites/cato.org/files/2022-07/PA_932_2.pdf.

25. Bank Policy Institute, *Getting to Effectiveness—Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance*, October 29, 2018, https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf.

26. Asli Demirgüç-Kunt et al., *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*, World Bank Group, 2022, 33, https://www.worldbank.org/en/publication/globalfindex.

27. One of the authors of this report, J. Christopher Giancarlo, is cofounder and executive chairman of the Digital Dollar Project, and the other author, Jim Harper, is a member of its advisory board.

28. Digital Dollar Project, Privacy Sub-Committee, "Privacy Principles for a Digital Dollar," October 18, 2021, https://digitaldollarproject.org/wp-content/uploads/2021/10/DDP-Privacy-Principles-10.18.21_Final.pdf.

29. See Jim Harper, "What Do People Mean by 'Privacy,' and How Do They Prioritize Among Privacy Values? Preliminary Results," American Enterprise Institute, March 18, 2022, https://www.aei.org/research-products/report/what-do-people-mean-by-privacy-and-how-do-they-prioritize-among-privacy-values-preliminary-results.

30. See Jim Harper, "Understanding Privacy—and the Real Threats to It," Cato Institute, August 4, 2004, https://www.cato.org/policy-analysis/understanding-privacy-real-threats-it.

31. See Oren Bar-Gill, Omri Ben-Shahar, and Florencia Marotta-Wurgler, "Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts," *University of Chicago Law Review* 84, no. 1 (Winter 2017): 7–35, https://chicagounbound.uchicago.edu/uclrev/vol84/iss1/2; and Gregory Klass, "Empiricism and Privacy Policies in the Restatement of Consumer Contract Law," *Yale Journal on Regulation* 36, no. 1 (Winter 2019): 45–115, https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3005&context=facpub.

32. Federal Reserve Bank of Boston, "Project Hamilton Phase 1 Executive Summary," February 3, 2022, https://www.bostonfed.org/publications/one-time-pubs/project-hamilton-phase-1-executive-summary.aspx.

33. The topmost "privacy" concern people cite when asked an open-ended question about privacy concerns is about financial security. Harper, "What Do People Mean by 'Privacy,' and How Do They Prioritize Among Privacy Values?"

34. Roger Lowenstein, *America's Bank: The Epic Struggle to Create the Federal Reserve* (New York: Penguin Books, 2015).

35. Admittedly, Americans already tolerate government agencies taking money out of their bank accounts, as evidenced by the increasing percentage of individual income tax paid to the IRS through its eFile System with tax payments and refunds processed directly through personal bank accounts. See Internal Revenue Service, "Income Tax Return, eFile Statistics," https://www.efile.com/efile-tax-return-direct-deposit-statistics.

36. During his presidency, Ronald Reagan notably adapted the Russian proverb, "*Doveryay, no proveryay*," when referring to arms treaty compliance by the United States and the Soviet Union. Barton Swaim, "'Trust, but Verify': An Untrustworthy Political Phrase," *Washington Post*, March 11, 2016, https://www.washingtonpost.com/opinions/trust-but-verify-an-untrustworthy-political-phrase/2016/03/11/da32fb08-db3b-11e5-891a-4ed04f4213e8_story.html?noredirect=on.

37. White House, Office of Science and Technology Policy, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.

38. White House, Office of Science and Technology Policy, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.

39. Vivek Ramaswamy and Jed Rubenfeld, "Twitter Becomes a Tool of Government Censorship," *Wall Street Journal*, August 17, 2022,

https://www.wsj.com/articles/twitter-becomes-a-tool-of-government-censors-alex-berenson-twitter-facebook-ban-covid-misinformation-first-amendment-psaki-murthy-section-230-antitrust-11660732095.

40. David Zweig, "How Twitter Rigged the Covid Debate," Free Press, December 26, 2022, https://www.thefp.com/p/how-twitter-rigged-the-covid-debate; Melissa Koenig, "Twitter Files Dump Shows Company Suppressed Debate and Information from Doctors and Experts Which Clashed with White House—and Suspended Vaccine Skeptic Alex Berenson at Biden's Request," *Daily Mail*, December 26, 2022, https://www.dailymail.co.uk/news/article-11574573/Twitter-suppressed-covid-information-doctors-experts.html; and Jennifer Sey, "The Twitter Files Reveal an Unholy Alliance," *Spectator*, December 26, 2022, https://thespectator.com/topic/twitter-files-show-unholy-alliance-state-corporate-power.

41. In October 2022, PayPal published and then rescinded a policy allowing it to levy fines of $2,500 for violating its acceptable use policy by promoting misinformation. Emily Mason, "After PayPal Revokes Controversial Misinformation Policy, Major Concerns Remain over $2,500 Fine," *Forbes*, October 27, 2022, https://www.forbes.com/sites/emilymason/2022/10/27/after-paypal-revokes-controversial-misinformation-policy-major-concerns-remain-over-2500-fine/?sh=152c4b7f30c4.

42. Operation Chokepoint was a US government initiative to pressure financial institutions into denying services to lawful but politically disfavored businesses, such as pawnshops, check cashers, and cannabis dispensaries. See Alan Zibel and Brent Kendall, "Probe Turns Up Heat on Banks," *Wall Street Journal*, August 7, 2013, https://www.wsj.com/articles/SB10001424127887323838204578654411043000772.

43. "We don't know who's using a $100 bill today and we don't know who's using a 1,000 peso bill today. The key difference with the CBDC is the central bank will have absolute control on the rules and regulations that will determine the use of that expression of central bank liability, and also we will have the technology to enforce that." Agustín Carstens, "Digital Currencies and the Soul of Money" (speech, Goethe University's Institute for Law and Finance, Frankfurt, Germany, January 18, 2022), https://www.bis.org/speeches/sp220118.htm.

44. Jack Schickler, "Digital Euro Will Have Privacy Safeguards, European Finance Ministers Say," CoinDesk, April 4, 2022, https://www.coindesk.com/policy/2022/04/04/digital-euro-will-have-privacy-safeguards-european-finance-ministers-say.

45. Federal Reserve Board, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, January 2022, https://www.federalreserve.gov/publications/january-2022-cbdc.htm.

46. White House, Office of Science and Technology Policy, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.

47. Other commentators also identify the potential use of privacy-enhancing technologies to enable privacy protection in digital currency. See Daniel Gorfine and Michael Mosier, "Opinion: Stablecoin and Other Digital Assets Are Falsely Framed as a Choice Between Personal Privacy and National Security. We Can Have Both.," MarketWatch, July 23, 2022, https://www.marketwatch.com/story/stablecoin-and-other-digital-assets-are-falsely-framed-as-a-choice-between-personal-privacy-and-national-security-we-can-have-both-11658206072.

48. As a regulator, coauthor Giancarlo initiated an approach to market regulation using big data techniques that he dubbed quantitative regulation or "QuantReg." See J. Christopher Giancarlo, "Quantitative Regulation: Effective Market Regulation in a Digital Era" (speech, Georgetown University Law School, Washington, DC, November 7, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo59?utm_source=govdelivery.

49. White House, Office of Science and Technology Policy, *Technical Evaluation for a U.S. Central Bank Digital Currency System*.